PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-290900**
(43)Date of publication of application : **04.10.2002**

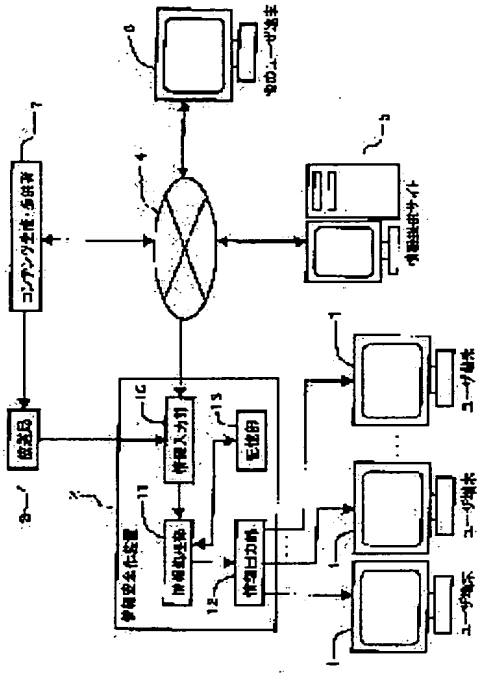
(51)Int.Cl. **H04N 5/91**
G06F 11/00
G06F 13/00
G06F 17/60

(21)Application number : **2001-085196**
(22)Date of filing : **23.03.2001**

(71)Applicant : **HITACHI LTD**
(72)Inventor : **SANO KENJI**

(54) INFORMATION SCREENING DEVICE AND INFORMATION GUARANTEE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent improper information from invading a user terminal which is arranged at home, etc.
SOLUTION: An information screening device 2 performs the unitary management of safety of information to be transmitted to a plurality of user terminals 1 and excludes improper information or adverse information, etc., at the border. Information transmitted from a broadcasting station 3 or an information providing site 5, etc., to the user terminals 1 is first received with the information input part 10 of the information screening device 2. Received information is checked with an information processing part 11 concerning a virus or contents. A screening processing such as the removal of virus data or the partial replacement of the contents is performed in improper information. The information processing part 11 gives a guarantee mark to information which is confirmed safe and an information output part 12 transmits the information to the user terminals 1.



LEGAL STATUS

[Date of request for examination] 27.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－290900
（P2002－290900A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04N	5/91		G06F	13/00	351Z　5B076
G06F	11/00			17/60	302E　5B089
	13/00	351	H04N	5/91	P　5C053
	17/60	302	G06F	9/06	660N

審査請求　未請求　請求項の数17　ＯＬ　（全 14 頁）

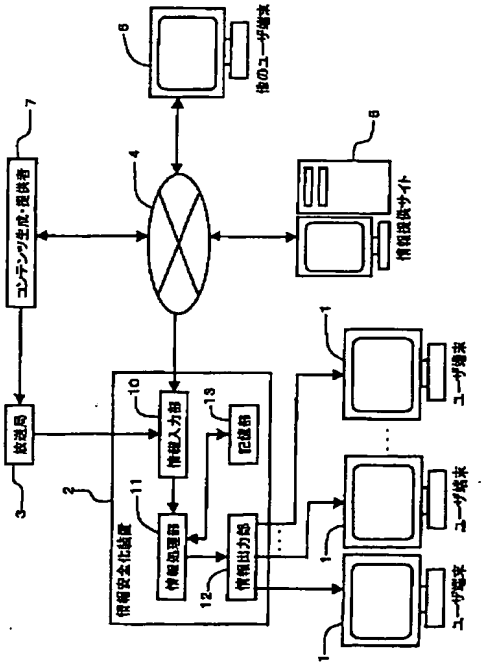
(21)出願番号　特願2001－85196(P2001－85196)
(22)出願日　平成13年３月23日(2001.3.23)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　佐野　賢治
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100095371
弁理士　上村　輝之　（外２名）

Ｆターム(参考)　5B076 FD08
5B089 GA11 GB02 KA17 KC47 KC51
KC52 KC53 KH28
5C053 FA15 LA06 LA11 LA14

(54)【発明の名称】　情報安全化装置及び情報保証システム

(57)【要約】
【課題】　家庭内等に設置されたユーザー端末に不適切な情報が侵入するのを未然に防止すること。
【解決手段】　情報安全化装置２は、複数のユーザー端末１へ送信する情報の安全性を一元的に管理し、水際で不適切な情報や悪質な情報等を排除するものである。放送局３や情報提供サイト５等からユーザー端末１に向けて送信された情報は、まず情報安全化装置２の情報入力部１０で受信される。受信された情報は、情報処理部１１によってウイルスチェックやコンテンツの内容チェックが行われる。不適切な情報には、ウイルスデータの駆除やコンテンツの一部置換等の安全化処理が施される。情報処理部１１は、安全が確認された情報に保証マークを与えて、情報出力部１２からユーザー端末１に送信させる。



1

【特許請求の範囲】

【請求項１】　情報を供給する情報供給源と前記情報を利用する情報端末との間に設けられる情報安全化装置であって、

前記情報供給源から通信ネットワークを介して情報を受信する受信手段と、

前記受信した情報がユーザーの望まない情報（以下、不要情報）であるか否かを検査し、前記情報が不要情報であると判定した場合には、予め設定された所定の安全化処理を施す情報処理手段と、

前記不要情報以外の情報であると判定された情報及び前記安全化処理が施された情報を、予め設定された所定の情報端末に送信させる送信手段と、を備えたことを特徴とする情報安全化装置。

【請求項２】　前記検査された情報に、検査済みの情報であることを示す保証情報を付加する保証情報付加手段を更に備えた請求項１に記載の情報安全化装置。

【請求項３】　保証情報が対応付けられた情報が編集処理された場合には、前記保証情報を無効とする請求項２に記載の情報安全化装置。

【請求項４】　前記情報処理手段は、前記保証情報が付加された情報については、前記不要情報以外の情報であると判定する請求項３に記載の情報安全化装置。

【請求項５】　前記保証情報は、該保証情報が付加された情報を前記情報端末で利用する際に、ユーザーが認識可能に出力されるものである請求項２～請求項４のいずれかに記載の情報安全化装置。

【請求項６】　前記安全化処理が施された情報に、安全化処理済みであることを示す処理済み情報を付加する処理済み情報付加手段を更に備えた請求項１～請求項５のいずれかに記載の情報安全化装置。

【請求項７】　前記処理済み情報は、該処理済み情報が付加された情報を前記情報端末で利用する際に、ユーザーが認識可能に出力されるものである請求項６に記載の情報安全化装置。

【請求項８】　前記不要情報とは、前記情報端末に悪影響を及ぼす可能性のあるデータであり、前記安全化処理は、前記データを駆除するものである請求項１～請求項７のいずれかに記載の情報安全化装置。

【請求項９】　前記安全化処理は、前記情報端末に送信される情報の連続性が失われないように、前記不要情報を無力化するものである請求項１～請求項７のいずれかに記載の情報安全化装置。

【請求項１０】　前記不要情報とは、閲覧が制限されている情報であり、前記安全化処理は、前記情報端末に送信される情報の連続性が失われないように、前記閲覧が制限されている情報を予め設定された置換用情報に置換するものである請求項９に記載の情報安全化装置。

【請求項１１】　前記不要情報とは、前記情報端末に悪影響を及ぼす可能性のあるデータ及び閲覧が制限されている情報であり、前記安全化処理は、前記情報端末に悪影響を及ぼす可能性のあるデータを駆除すると共に、前記情報端末に送信される情報の連続性が失われないように、前記閲覧が制限されている情報を予め設定された置換用情報に置換するものである請求項１～請求項７のいずれかに記載の情報安全化装置。

2

【請求項１２】　前記情報処理手段は、前記不要情報以外の情報であると判定された情報及び前記安全化処理が施された情報を前記情報端末が選択して受信するためのメニュー情報を生成し、前記情報端末に提供する請求項１～請求項１１のいずれかに記載の情報安全化装置。

【請求項１３】　前記情報処理手段は、予め登録された各ユーザーの情報端末にそれぞれ送信する情報を該各ユーザーが予め指定した条件に応じてそれぞれ検査し、所定の安全化処理を施すものである請求項１～請求項１２のいずれかに記載の情報安全化装置。

【請求項１４】　ユーザーの望まない可能性のある情報（以下、不要情報）を含むコンテンツデータの生成方法であって、

時間圧縮された不要情報を生成するステップと、

前記不要情報を特定するための情報を該不要情報に対応付けるステップと、

前記不要情報に置換されるべき置換用情報を、前記不要情報の再生時間と同一時間となるように時間圧縮して生成するステップと、

前記不要情報と前記置換用情報とを対応付けるステップと、を含んでなるコンテンツデータの生成方法。

【請求項１５】ユーザーの望まない可能性のあるデータ（以下、不要データ）を時間圧縮して記録する第１の記録領域と、

前記第１の記録領域に対応付けて設けられ、前記不要データを特定するためのデータを記録する第２の記録領域と、

前記第１の記録領域に続けて設けられ、前記不要データに置換されるべき置換用データを、前記不要データの再生時間と同一時間となるように時間圧縮して記録する第３の記録領域と、を有するコンピュータ読取り可能な記録媒体。

【請求項１６】　情報供給源から各情報端末に配信される情報の安全性を保証するための情報保証システムにおいて、

前記情報供給源と前記各情報端末との間には、該各情報端末へそれぞれ配信される情報の安全性を一元的に確認するための情報安全化装置を設け、

前記情報安全化装置は、

前記情報供給源から通信ネットワークを介して情報を受信する受信手段と、

予め各ユーザーがそれぞれ設定した検査条件に基づいて、前記受信した情報がユーザーの望まない情報（以下、不要情報）であるか否かを検査し、不要情報である

場合は予め設定された所定の安全化処理を施すと共に、
前記検査又は安全化処理により安全であると判定した情報に保証情報を対応付けて出力する情報処理手段と、
前記情報処理手段により安全であると判定された情報及び前記保証情報を、前記各情報端末に向けてそれぞれ送信される送信手段と、を備えて構成したことを特徴とする情報保証システム。

【請求項１７】 情報供給源から情報端末へ配信される情報の安全性を、該情報端末が受信する前に検査するためのコンピュータプログラムにおいて、
前記情報供給源から通信ネットワークを介して情報を受信させる機能と、
前記受信された情報がユーザーの望まない情報（不要情報）であるか否かを検査する機能と、
前記受信された情報が前記不要情報であると判定された場合には、予め設定された所定の安全化処理を施す機能と、
前記受信した情報が前記不要情報以外の情報であると判定された場合には、該情報に保証情報を対応付ける機能と、
前記保証情報が対応付けられた情報を前記情報端末に送信させる機能と、をコンピュータ上に実現させるためのコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザーが利用する各種の情報端末に供給される情報の安全性を事前に検査し、必要な安全化処置を施してから前記情報端末に送信させる情報安全化装置及び情報保証システムに関する。

【０００２】

【従来の技術】ユーザーは、例えば、テレビジョン受像機、パーソナルコンピュータ、携帯情報端末（携帯電話を含む）等のような各種の情報端末を用いることにより、ネットワークを介して供給される各種のコンテンツを閲覧し、利用等することができる。しかし、各種のコンテンツの中には、ユーザーにとって好ましくないものも存在する。

【０００３】例えば、インターネット等の広域大規模通信ネットワークを介して、電子メールをやり取りしたり、無償又は有償で配布されているプログラムやコンテンツ（映像等）をダウンロードしたりする場合を例に挙げると、受信したデータ（プログラムを含む）中に、いわゆるコンピュータウイルスが含まれていることもある。

【０００４】また、例えば、テレビ放送を例に挙げると、受信した映像の一部又は全部に、過激な暴力場面や性的描写場面が含まれていることがあるが、このような刺激の強い場面の映像は、全てのユーザーに受け入れられるわけではない。例えば、青少年のいる家庭では、このような映像の視聴を望まない。

【０００５】そこで、従来は、例えば、情報端末にインストールされたいわゆるワクチンソフトによって、情報端末が受信した情報ファイルのウイルス感染を検査している。また、放映される場面がユーザーにとって適正なものであるか否かについては、保護者等が予め放送内容を視聴して判断し、不適切と判断した場面について外部操作により視聴を規制する技術も知られている。

【０００６】

【発明が解決しょうとする課題】ユーザーは、受信した情報がコンピュータウイルスに感染しているか否か予め知ることができないので、全ての受信情報について検査する必要がある。即ち、たとえ情報供給元の信頼性が高い場合であっても、受信情報の安全性についてユーザー側では確認できないため、全ての受信情報を検査しなければならない。また、ウイルスパターンは、日々変化するため、ユーザーは、常に最新のウイルス情報を入手してワクチンソフトを更新しなければならない。このため、ユーザー側の作業が煩雑化し、使い勝手が悪い。

【０００７】一方、予め放送内容を視聴し、不適切と判断した場面について外部操作により視聴を規制する方法では、ユーザーの作業が煩雑であり、やはり使い勝手が低い。また、過激な場面の終了を予測するのが難しく、視聴可能な場面まで規制される可能性もある。

【０００８】さらに、近年では、テレビジョン放送とデータ通信とが融合したり、インターネット接続の可能なテレビジョン受像機やテレビ放送が視聴可能なパーソナルコンピュータ等が普及している。また、一家に一台の情報端末を所有する時代から一人一台の時代を経て、一人が複数種類の情報端末を所有する時代を迎えている。従って、ユーザー、特に、未成年の家族と同居する親や教育者あるいは監督者等は、多種類の情報端末を介して配信される多くの受信情報の全てについて、その安全性を事前に確認する必要があり、大変煩雑な作業を強いられる。

【０００９】本発明は、上述した種々の問題に鑑みてなされたもので、その目的は、情報端末に受信される前に、該情報端末に配信された情報の安全性を確認するための情報安全化装置及び情報保証システムを提供することにある。本発明の他の目的は、安全性が確認された情報に保証を与え、安全な情報の流通を円滑化できるようにした情報安全化装置及び情報保証システムの提供にある。本発明の更なる目的は、後述する実施の形態の記載から明らかになるであろう。

【００１０】

【課題を解決するための手段】上記課題を解決するために、本発明に係る情報安全化装置は、情報を供給する情報供給源と情報を利用する情報端末との間に設けられる。この情報安全化装置は、情報供給源から通信ネットワークを介して情報を受信する受信手段と、受信した情

報がユーザーの望まない情報（以下、不要情報）であるか否かを検査し、不要情報であると判定した場合には、予め設定された所定の安全化処理を施す情報処理手段と、不要情報以外の情報であると判定された情報及び安全化処理が施された情報を、予め設定された所定の情報端末に送信させる送信手段とを備える。

【００１１】ここで、「情報」としては、例えば、地上波や衛星又はケーブル等を介したテレビジョン放送の放映内容、インターネット等を利用する電子メール、ウェブページ、プログラム、映像データ、音楽データ等の種々のものを挙げることができる。従って、「情報供給源」としては、例えば、テレビ局、ウェブサイト、ネットワークに接続された他の情報端末等を挙げることができる。「ユーザーの望まない情報」とは、積極的又は消極的にユーザーが受信を希望しない情報の意味であり、具体的には、例えば、情報端末に悪影響を及ぼすおそれのあるプログラムやデータ（いわゆるコンピュータウイルス）や、未成年者等に視聴が規制されている過激な場面の映像や音声等のような不適切な情報、不適正な情報、悪質な情報を挙げることができる。

【００１２】情報安全化装置は、情報端末と情報供給源との間に位置して、情報端末が情報を受信する前に、全ての情報の安全性を検査する。不要情報の場合は、所定の安全化処理を施してから情報端末に送信する。これにより、情報端末を利用するユーザー自身は、ウイルス情報の更新や、好ましくない場面の事前検閲等を行う必要がない。

【００１３】好適な実施形態によれば、保証情報付加手段は、検査された情報に検査済みの情報であることを示す保証情報を付加する。

【００１４】そして、保証情報が付された検査済みの情報がユーザーの情報端末で編集処理された場合には、保証情報は無効とされる。検査済みの情報に操作が加えられることにより、安全性を保証し得なくなるためである。ここで、保証情報を無効にするとは、例えば、保証情報を削除する場合のほか、保証情報自体は存続させて有効性を示す値を０に設定する場合も含む。

【００１５】検査後に操作が加えられた場合に保証情報を無効とすることにより、保証情報に対する信頼性がより高まる。そこで、情報処理手段は、保証情報が付加された情報については、不要情報以外の情報であると直ちに判定することができる。例えば、ある一群の情報端末の安全性を一元的に管理する情報安全化装置によって検査され保証情報が付加された情報が、他の一群を構成する情報端末に転送された場合、該他の一群の情報端末の安全性を統括する情報安全化装置では、何ら検査することなく、この保証情報付きの情報を安全なものとして受け入れることが可能である。

【００１６】好適な実施形態では、保証情報は、該保証情報が付加された情報を情報端末で利用する際に、ユーザーが認識可能に出力される。「ユーザーが認識可能に出力」とは、ユーザーが五官で保証情報の存在を感知できるように出力することを意味し、具体的には、例えば、ディスプレイ装置に表示出力されるマークやコメント、スピーカーに音声出力される鳴動音やメッセージ等を挙げることができる。

【００１７】また、不要情報を無力化する安全化処理が施された情報についても、安全化処理済みであることを示す処理済み情報を付加することができる。そして、この処理済み情報もユーザーが認識可能に出力するのが好ましい。

【００１８】好適な実施形態では、安全化処理は、情報端末に送信される情報の連続性が失われないように、不要情報を無力化するようになっている。「情報の連続性が失われないように」とは、情報端末が既に受信した部分とこれから受信する部分との時間経過上の連続性、一体性が損なわれないようにすることを意味する。

【００１９】例えば、不要情報として、閲覧が制限されている情報を挙げると、安全化処理は、情報端末に送信される情報の連続性が失われないように、閲覧が制限されている情報を予め設定された置換用情報に置換する。なお、置換用情報は、閲覧が制限されている情報と同一の再生時間となるように圧縮されているのが好ましい。さらに、置換用情報は、例えば、過激な情景描写を廃し、ストーリーの把握に支障を与えないような情報として加工されているのがより望ましい。

【００２０】好適な実施形態では、検査済み又は安全化処理済みの情報は、無条件で直ちに情報端末に送信されるのではなく、受信情報を選択するためのメニュー情報に基づいて、ユーザーは、受信を希望する情報を選択するようになっている。

【００２１】好適な実施形態によれば、情報処理手段は、予め登録された各ユーザーの情報端末にそれぞれ送信する情報を該各ユーザーが予め指定した条件に応じてそれぞれ検査し、所定の安全化処理を施すようになっている。

【００２２】本装置によるサービスを希望する各ユーザーは予め登録する必要がある。各ユーザーは、情報の安全性に関する条件をそれぞれ指定できる。具体的には、例えば、「成人指定」等のような視聴規制のある放送内容の場合、各情報端末を利用する視聴者の年齢層によって、安全性の判断は異なる。そこで、情報処理手段は、各ユーザーが予め登録した条件に基づいて、安全性をそれぞれ判断する。本装置によるサービスの開始及び停止は、各ユーザーがそれぞれ自由に設定することが可能である。

【００２３】時間圧縮された不要情報を生成するステップと、不要情報を特定するための情報を該不要情報に対応付けるステップと、不要情報に置換されるべき置換用情報を、不要情報の再生時間と同一時間となるように時

間圧縮して生成するステップと、不要情報と置換用情報とを対応付けるステップとによって、不要情報を含んだコンテンツデータを生成することができる。

【００２４】不要情報と置換用情報とを時間圧縮することにより、圧縮情報を伸長して再生する時に生じる時間差分を利用して、時間の連続性を損なわずに不要情報を置換用情報に置き換えることができる。どの部分が不要情報であるかを特定するための情報は、コンテンツデータの先頭に設けてもよいし、不要情報の先頭に設けてもよい。不要情報を特定するための情報を検出することにより、不要情報を置換用情報に置き換えることができる。

【００２５】

【発明の実施の形態】以下、図１～図１１に基づき、本発明の実施の形態を説明する。図１は、情報安全化装置を備えた情報保証システムの全体を概略的に示す構成説明図である。

【００２６】各ユーザーの使用する「情報端末」としてのユーザー端末１は、情報安全化装置２にそれぞれ接続されている。ユーザー端末１としては、例えば、テレビジョン受像機、パーソナルコンピュータ、携帯情報端末（携帯電話を含む）等を挙げることができる。各ユーザー端末１は、少なくとも出力手段及び操作手段をそれぞれ備えている。出力手段としては、例えば、モニタディスプレイ装置やスピーカ等を挙げることができる。操作手段としては、例えば、キーボードスイッチ、ポインティングデバイス、マイクロフォン等を挙げることができる。ユーザー端末１がパーソナルコンピュータやワークステーション又は携帯情報端末のようなマイクロコンピュータシステム製品として構成される場合、該ユーザー端末１は、情報安全化装置２を経由して受信した情報を編集したり、新たな情報を生成して発信することもできる。

【００２７】各ユーザー端末１は、情報安全化装置２を介してテレビ放送やインターネットからのデータ等を受信する。情報安全化装置２は、予め登録された複数のユーザー端末１へ送信する情報の安全性をそれぞれ個別に管理することができる。例えば、集合住宅の各家庭にそれぞれ設置されたユーザー端末１を一台の情報安全化装置２によって管理できるし、または、一家庭内に設置された複数のユーザー端末１を家庭内に設置した情報安全化装置２によって管理することもできる。これに限らず、各ユーザー端末１毎に情報安全化装置２を設ける構成としてもよい。

【００２８】情報安全化装置２は、各ユーザー端末１へ不適切、不適正な情報が配信されるのを水際で防止すべく、各ユーザー端末１と通信ネットワーク４との間に設けられる。通信ネットワーク４としては、例えば、公衆電話回線等を使用したインターネット網を挙げることができる。また、情報安全化装置２は、衛星通信や地上波又はケーブル伝送等を介して、「情報供給源」の一つである放送局３が放映する番組を受信することができる。

【００２９】通信ネットワーク４には、「情報供給源」としての情報提供サイト５，他のユーザー端末６及びコンテンツ生成・提供者の装置（以下「コンテンツ提供装置」）７が接続されている。情報提供サイト５は、例えば、HTMLやXML等で記述されたウェブページやプログラム等の各種情報をHTTPやFTP等の所定のプロトコルにより提供する。他のユーザー端末６としては、例えば、パーソナルコンピュータやワークステーションあるいは携帯情報端末等を挙げることができる。他のユーザー端末６から情報安全化装置２の管理下にある各ユーザー端末１に向けて電子メール等の情報を送信することができる。コンテンツ提供装置７は、例えば、映画やドラマ又はニュース等の各種映像番組、音楽番組、ラジオ番組を生成して配信するものである。コンテンツ提供装置７が提供する各種のコンテンツは、通信ネットワーク４を介して、又は放送局３から情報安全化装置２に送信される。

【００３０】次に、情報安全化装置２の構成について、図１及び図２を参照しつつ説明する。情報安全化装置２は、「受信手段」としての情報入力部１０と、「情報処理手段」としての情報処理部１１と、「送信手段」としての情報出力部１２と、「記憶手段」として表現可能な記憶部１３とから大略構成されている。

【００３１】情報入力部１０は、例えば、テレビ放送やデータ通信等の各種情報を受信可能に構成されており、各ユーザー端末１宛の情報をそれぞれ並列に受信処理可能である。情報処理部１１は、コンピュータ資源を利用して、受信した情報の安全性を検査し、ユーザーの望まない不適切又は不適正な情報（不要情報）を安全化するものである。

【００３２】図２に示すように、情報処理部１１は、「検査手段」として表現可能な検査部２１と、「安全化処理手段」として表現可能な安全化処理部２２と、「保証情報付加手段」及び「処理済み情報付加手段」としての保証マーク付与部２３とを備えている。

【００３３】検査部２１は、受信した情報の安全性を検査するものである。検査部２１は、各ユーザーが予め設定した検査条件に基づいて、各受信情報の安全性をそれぞれ判断する。ユーザー毎の検査条件は、記憶部１３内に形成されるユーザー管理データベースで管理することができる。ここで、検査部２１は、各ユーザーの指定した検査条件に無条件で従う必要はない。例えば、受診情報がコンピュータウイルス等のようにコンピュータ資源に致命的な悪影響を与える可能性を有する場合は、ユーザー指定条件にかかわらず、不要情報であると判定することができる。

【００３４】検査部２１は、各受信情報の特性（性質、種類）に応じて安全性をそれぞれ判断するものである。

例えば、データ（プログラムを含む）を受信した場合、検査部２１は、この受信データ中に予め登録されたウイルスパターンが存在するか否かをパターンマッチング法等によって検査する。ウイルスチェックに用いるウイルスパターンデータは、記憶部１３内に形成されるウイルス管理データベースで管理することができる。なお、このウイルス管理データベースは、定期的に又は不定期に最新の情報に自動更新される。ウイルスパターンの更新は、ウイルスパターンを提供する情報提供サイト５からの通知（プッシュ型更新）、又はウイルス管理データベースから情報提供サイト５への最新ウイルスパターンの問合せ（プル型更新）等により行うことができる。また、ウイルスを含むデータを通信ネットワーク４から受信した場合、検査部２１は、ウイルスを含有するデータの送信元やウイルス情報を管理するサイト等に対して警報メッセージを送信する機能を有する。

【００３５】テレビ放送や通信ネットワーク４から映像情報を受信した場合、検査部２１は、後述するように、不要情報の存在を示すランク情報の有無を検出し、ランク情報を検出した場合は、不要情報であると判定する。また、検査部２１は、検査済み又は安全化処理済みであることを示す保証マークが付加された情報については、不要情報以外の情報として、即ち安全な情報であると判断する。

【００３６】安全化処理部２２は、各受信情報の特性に応じた安全化処理を行うものである。例えば、不要情報がコンピュータウイルス等のように、本来の情報に付加された冗長な情報である場合、安全化処理部２２は、冗長な情報を削除することにより安全化処理を施す。例えば、映像の一部に過激な場面等の不要情報が存在する場合、安全化処理部２２は、後述のように、不要情報に対応付けられている置換用情報で不要情報を置き換えることにより安全化処理を施す。安全化処理部２２は、圧縮された情報をソフトウエア又はハードウエアによって伸長させる伸長手段を備えている。なお、映像等の圧縮情報は、いったん記憶部１３内のコンテンツ格納部に蓄積させてから伸長することができる。

【００３７】保証マーク付与部２３は、検査部２１によって安全であると判定された情報及び安全化処理部２２によって安全化処理された情報について、情報の安全性を示す保証マークを付加するものである。図３と共に後述するように、保証マークのデータには、コピー管理データが付随する。保証マークが対応付けられた情報がユーザー端末１上で編集処理された場合は、保証マークは無効となる。ここで、留意すべき点は、保証マーク付与部２３は、予め用意された複数種類の保証マークデータのうち、受信情報の特性に応じて一又は複数の保証マークを付加させる点である。例えば、コンピュータウイルスが含まれていない情報に対しては「ウイルス検査済みマーク」を、ウイルスが除去された情報については「ウイルス除去済みマーク」を、過激な場面を穏当な置換用情報に置き換えた場合は「置換済みマーク」を、それぞれ付加することができる。映像が通信ネットワーク４を介してデータ通信で配信された場合には、例えば「ウイルス検査済みマーク」と「置換済みマーク」のように、一つの情報に複数種類のマークが付加される場合もある。

【００３８】情報出力部１２は、安全であると判定された情報及び安全化処理された情報を、予め登録された所定のユーザー端末１に向けて送信する。即ち、情報出力部１２は、安全な情報のみを各ユーザー端末１に送信する。また、情報出力部１２は、予め情報保証サービスを申し込んでいるユーザーの端末１に対してのみ情報を送信する。情報出力部１２と各ユーザー端末１とは、例えば、有線又は無線式のLAN（Local Area Network）、公衆電話回線網等の種々の通信媒体を介して接続可能である。

【００３９】情報安全化装置２は、上述の構成に加えて、各ユーザー端末１からの情報転送要求を処理するための手段も備えている。情報要求受付部３１は、例えば、テレビチャンネルの番号、URL（Uniform Resource Locator）、電子メールアドレス、電話番号等の各種情報取得に必要な要求を各ユーザー端末１からそれぞれ受け付けるものである。受け付けられた情報転送要求は、情報要求発行部３２により所定の情報供給源に送られる。

【００４０】次に、図３及び図４を参照して、データ構造等につき説明する。まず、図３は、検査済み又は安全化処理済みの情報（コンテンツ）に保証マークを対応付けて送信する場合のデータ構造を概略的に示す模式図である。

【００４１】情報処理部１１が出力するデータは、図３（ａ）に示すように、４種類のデータ記憶領域Ｄ１～Ｄ４を有する。先頭に位置する識別データ領域Ｄ１には、検査等された情報の供給元を特定する情報と、宛先のユーザー端末１を特定する情報と、データ種別を示す情報と、データ長を示す情報等の識別データが格納されている。マークデータ領域Ｄ２には、保証マーク付与部２３により付加された一つ又は複数の保証マークのデータが格納されている。なお、保証マークのデータ自体を直接格納するのではなく、ユーザー端末１側に予めインストールされた保証マークのデータを特定するための情報でもよい。コピー管理領域Ｄ３には、保証マークのコピー制限を行うためのデータが格納されている。検査済み又は安全化処理済みのコンテンツが編集処理され改変された可能性がある場合、コピー管理データは「コピー不可」にセットされる。これにより、編集処理されたコンテンツに保証マークデータは付加されない。コンテンツの編集処理を行わず、ユーザー端末１側のローカルディスクに単純に記憶させたような場合は、コンテンツ再生

時に保証マークのデータも再現される。なお、コピー管理データによって、コンテンツの著作権管理を併せて行うようにしてもよい。

【００４２】図３（ｂ）には、ユーザー端末１側での表示状態の一例が示されている。ユーザー端末１のディスプレイ装置には、検査済み又は安全化処理済みのコンテンツが保証マークと対応付けられて一覧形式で表示される。即ち、図３（ｂ）は、受信を希望するコンテンツを選択する選択メニュー画面であって、保証マークとコンテンツ名とを対応付けて一覧表示させることにより、ユーザーは、情報受信前に、コンテンツの内容や安全性等を予め確認することができるようになっている。ユーザーは、一覧表示された各コンテンツの中から、受信を希望するコンテンツを選択することができる。例えば、ダイレクトメールと思われる場合、ユーザーは、このコンテンツの受信を拒否することができる。ユーザーがコンテンツを選択すると、保証マークと共に、コンテンツの内容がディスプレイ装置に表示される。保証マークは、コンテンツの視聴を妨げないように、目立たない位置に表示させることができる。また、保証マークは、コンテンツの視聴中に常時表示させても良いし、最初の所定時間だけ表示させてもよい。

【００４３】次に、図４は、閲覧が規制されている情報を含むコンテンツのデータ構造及び再生方法を概略的に示す説明図である。

【００４４】ここで、図中に示すオリジナルデータＤＡ～ＤＣとは、映像等のオリジナル場面のデータであり、それぞれデジタル化されて時間圧縮されている。ランク情報とは、過激な場面等の視聴に不適切な部分を特定するための情報であり、ランク付けの情報（例えば、１３歳未満視聴不可、１８歳未満視聴不可、２０歳以上視聴可等）と、不適切なデータの範囲を特定するための情報（例えば、バケット番号やデータ長等）と、ランク情報に対応するランク対応情報（Ｄ１４）を特定するための情報とを備えている。図４の例では、オリジナルデータＤＢを規制されるべき場面のデータとして示している。ランク対応情報は、規制されるべきデータに置換するための置換用データＤＢＸを識別するものである。

【００４５】図４（ａ）に示すように、ユーザーが予め設定した条件、即ち視聴ランクがランク情報中のランクよりも高い場合は、オリジナルデータＤＡに続いて、オリジナルデータＤＢが伸長され、ユーザー端末１に配信される。逆に、ユーザーの設定した視聴ランクがランク情報中のランクよりも低い場合は、オリジナルデータＤＢに代えて、置換用データＤＢＸが伸長されてユーザー端末１に配信される。

【００４６】ここで、注意すべき点は、オリジナルデータＤＢと置換用データＤＢＸとは、伸長して再生される開始時刻（Ｔ０）、終了時刻（Ｔ１）、再生時間（Ｔ０－Ｔ１）が同一となるように設定されている点である。各データＤＡ～ＤＣ及びＤＢＸは、それぞれ圧縮された状態で情報供給源から受信されるため、非圧縮状態のデータを再生する時間と圧縮データを伸長して再生する時間との差分を利用して、置換データＤＢＸの開始時刻及び終了時刻をオリジナルデータＤＢのそれと一致させることができる。これにより、コンテンツの再生時間経過上の連続性は保持される。

【００４７】なお、これに限らず、置換データＤＢＸは、オリジナルデータＤＢとは別にして受信しておき、置換時に入れ替えるようにしてもよい。この場合は、各データを圧縮する必要はない。また、各データがバケット化されている場合は、各バケットにバケットデータの属性を示す情報（オリジナルデータか置換用データか）と、ランク情報（オリジナルデータのバケットのみ）と、オリジナルデータのどのバケットに対応するのかを示す情報（置換用データのバケットのみ）等の識別データをそれぞれ付加しておけばよい。この識別データによってバケットを分別し、ユーザーの設定したランクに応じてデータの入れ替え処理を行うことができる。ユーザーの設定したランクが低い場合、識別データ中にランク情報の設定されていないバケットはそのまま伸長して再生し、ランク情報の設定されたバケットは破棄し、置換用データのバケットのみを選択して伸長再生すればよい。

【００４８】置換用データの内容としては、種々のものを採用することができる。「１３未満の視聴が規制されています」等のメッセージを表示させるだけでも良いが、視聴規制に触れない範囲内で、ストーリー等の流れが把握できるような穏当な内容として置換用データを構成するのが好ましい。具体的には、視覚的に刺激的な場合は、アニメーション化したり、ワイヤーフレームモデルで表現することにより、ストーリーの連続性を保持したまま穏当な内容に変更することが可能である。聴覚的に刺激的な場合は、音声の一部消去や吹き替え、字幕等で対応可能である。

【００４９】次に、図５～図９に基づいて、本実施の形態の処理の流れを説明する。まず、図５は、受信情報中にコンピュータウイルスが含まれていた場合の説明図である。

【００５０】ユーザーが、端末１を介して電子メールやプログラム等の情報取得を情報安全化装置２に要求すると（Ｐ１）、この情報転送要求は情報安全化装置２を介して所定の情報供給源に送信される（Ｐ２）。情報供給源から送信された情報を情報安全化装置２が受信すると（Ｐ３）、情報安全化装置２は、受信情報を検査する（Ｐ４）。検査の結果、コンピュータウイルスが検出された場合は、情報安全化装置２によってウイルスが駆除されると共に（Ｐ５）、情報安全化装置２から情報供給源や関係機関に対してウイルス発見の警告メールが送信される（Ｐ６）。

【００５１】情報安全化装置２は、ウイルスを駆除した情報に保証マークを付加して（Ｐ７）、ユーザー端末１に送信する（Ｐ８）。次に、ユーザー端末１により発行された新たな情報転送要求に応じて（Ｐ９，Ｐ１０）、情報供給源から情報安全化装置２に送信された情報に保証マークが付加されている場合（Ｐ１１）、情報安全化装置２は、保証マークの有無だけを検査し（Ｐ１２）、この受信情報をユーザー端末１に送信する（Ｐ１３）。

【００５２】図６は、過激な場面等を含んだ映像等の情報を処理する場合の説明図である。ユーザーからの情報転送要求に応じて（Ｐ２１，Ｐ２２）、情報供給源から情報安全化装置２に圧縮された映像情報が送信される（Ｐ２３）。情報安全化装置２は、ユーザーが予め設定したランクに基づいて、受信した映像情報をそのまま配信するか否かを判定する（Ｐ２４）。ランク情報が設定されていない映像情報については、安全化処理部２２により圧縮映像情報を伸長してユーザー端末１に送信する（Ｐ２５，Ｐ２６）。一方、ランク情報の設定された映像情報及び該映像情報に置換される置換用情報が、情報供給源から情報安全化装置２に送信されて場合は（Ｐ２７，Ｐ２８）、映像情報中のランク情報を検査し（Ｐ２９）、ユーザー設定ランクよりも映像情報の設定ランクの方が高い場合は、置換用情報に入れ替る（Ｐ３０）。そして、置換用情報に保証マークを付加して（Ｐ３１）、ユーザー端末１に送信する（Ｐ３２）。

【００５３】次に、図７～図９は、処理の流れを示すフローチャートである。なお、これらの各フローチャートは、処理の概要を示すもので、実際のプログラム構造とは相違する。

【００５４】図７は、コンピュータウイルスをチェックするための処理を示す。まず、通信ネットワーク４を介して電子メールやウェブページ又はプログラム等のコンテンツを受信すると（Ｓ１）、この受信したコンテンツに保証マークの一種である検査済みマークが付加されているか否かを検査する（Ｓ２）。検査済みマークが付加されている場合（S2:YES）は、後述のＳ３～Ｓ８の各ステップを省略してＳ１０に移行する。一方、受信したコンテンツに検査済みマークが付加されていない場合は、既知のウイルスパターンとのパターンマッチングが行われる（Ｓ３）。

【００５５】パターン照合によりコンピュータウイルスが検出されなかった場合（S4:NO）は、検査済みマークを付加する（Ｓ５）。コンピュータウイルスが検出された場合は（S4:YES）、このウイルスを除去し（Ｓ６）、保証マークの一種である処理済みマークをコンテンツに付加する（Ｓ７）。そして、付加されたマークにコピー制限の情報を更に設定し（Ｓ８）、保証マークとコンテンツを対応付けて（Ｓ９）、受信選択用のメニューを生成し（Ｓ１０）、この受信選択用メニューをユーザー端末１に送信する（Ｓ１１）。ユーザーがメニューに基づいて受信を希望する情報を選択すると（S12:YES）、ユーザーにより選択された情報のみがユーザー端末１に送信される（Ｓ１３）。なお、ユーザーにより選択されなかった情報は、ユーザーからの指示に基づいて破棄することもできるし、所定期間だけ記憶部１３に保存した後、自動的に破棄することもできる。

【００５６】次に、図８は、視聴が規制されている場面を含んだ映像等のコンテンツを配信する場合の処理を示す。

【００５７】まず、通信ネットワーク４を介して映像データを受信すると（Ｓ２１）、受信データ中にランク情報が設定されているか否かを検査する（Ｓ２２）。ランク情報が設定されていない場合（S22:NO）は、穏当な内容のデータであるから、Ｓ２５に移行して受信データを伸長させる。ランク情報が付加されている場合は、ランク情報中の規制ランクとユーザーが設定したランクとを比較し、規制ランクがユーザー設定ランクを上回っているか否かを判定する（Ｓ２３）。規制ランクの方が高く設定されている場合は、置換用データに入れ替えて（Ｓ２４）、伸長処理を行う（Ｓ２５）。伸長されたデータは、送信タイミングが到来したときにユーザー端末１に送信される（Ｓ２６，Ｓ２７）。

【００５８】次に、図９は、ユーザー端末１側の受信処理を示す。まず、ユーザー端末１は、情報安全化装置２が提供する受信選択用のメニュー情報を受信する（Ｓ３１）。

【００５９】ユーザーは、表示されたメニューに基づいて（Ｓ３２）、受信を希望するコンテンツを選択する（Ｓ３３）。ユーザーがコンテンツを選択すると、この選択されたコンテンツの転送が情報安全化装置２に要求される（Ｓ３４）。情報安全化装置２からコンテンツを受信すると（S35:YES）、受信されたコンテンツがユーザー端末１のディスプレイ装置に表示される（Ｓ３６）。コンテンツの閲覧を終えたユーザーは、閲覧終了に際して、コンテンツデータをユーザー端末１のローカルディスクに保存するか否かを選択することができる（Ｓ３７）。コンテンツを保存する場合、コンテンツが編集されたか否かを判定し（Ｓ３８）、編集されていた場合（S38:YES）、保証マークを無効にすべくコピー管理情報を「コピー不可（禁止）」に設定させる（Ｓ３９）。

【００６０】このように構成される本実施の形態によれば、以下の効果を奏する。

【００６１】ユーザー端末１が情報を受信する前に、情報安全化装置２によって情報の安全性を検査し、必要な安全化処理を行うため、ユーザー端末１側でウイルスチェックやウイルスパターンデータの更新作業等を行う必要がない。これにより、ユーザー側での煩雑な作業を廃して、安全な情報のみを受信することができ、使い勝手が向上する。

【００６２】検査済みマーク、安全化処理済みマーク等の保証マークが付加された情報を情報安全化装置２からユーザー端末１に送信するため、保証マークによってユーザーに安心感や信頼感を与えることができる。

【００６３】検査等された情報が編集処理された場合は、保証マークを無効とするため、保証マークの信頼性を高めることができ、ひいては、保証マークの付加された情報についての実質的な検査を省略して速やかに情報をユーザー端末１に送信することができる。

【００６４】コンピュータウイルス及びテレビ放送という異なる種類の情報を情報安全化装置２で処理できるため、システムをコンパクトに構成することができ、使い勝手も高まる。

【００６５】安全性が確認された情報を直ちにユーザー端末１に送信するのではなく、受信選択用メニューを介してユーザーが選択した情報を情報安全化装置２からユーザー端末１に送信するため、ウイルスチェック等では排除しきれない不要な情報をユーザーの判断によって排除することができ、使い勝手が向上する。

【００６６】予め情報保証サービスを希望している複数のユーザー端末１への情報配信を一台の情報安全化装置２によって一元的に管理できるため、図１０に示すように、情報保証サービス停止中のユーザー端末１については、情報安全化装置２による保証は行われない。換言すれば、各ユーザー端末１は、情報安全化装置２をいわゆるレンタルファイアウォールのように利用することができる。即ち、各ユーザーは、必要と判断するときだけ、情報保証サービスを利用することが可能である。但し、実施の形態の記載から明かなように、本発明の情報安全化装置２は、単なるファイアウォールとは異なり、種々の利点を備えている点に注意すべきである。

【００６７】図１１に示すように、例えば、情報安全化装置２をISP（Internet Service Provider）の装置４１に設置し、インターネット接続契約を結んだユーザーを管理する顧客データベース４２と連動させることにより、ユーザー端末１は、公衆電話回線網（PSTN）４３等を介して安全な情報のみを受信することができる。

【００６８】次に、図１２に基づいて本発明の第２の実施の形態を説明する。図１２は、ユーザーによっては規制されるべき不適切な場面を含んだコンテンツを、本情報保証サービスで利用可能な形態で生成する場合の処理の流れを概略的に示すものである。

【００６９】まず、映画やドラマ等のコンテンツを生成した後（Ｓ４１）、このコンテンツの内容をチェックして規制すべき場面にランク情報を対応付ける（Ｓ４２）。次に、ランク情報が対応付けられた場面のデータに入れ替えるべき置換用データを生成する（Ｓ４３）。そして、オリジナルのデータと置換用データとを対応付けた後（Ｓ４４）、コンテンツを保存し、通信媒体や記録媒体を介して供給する（Ｓ４５）。

【００７０】なお、本発明は、上述した実施の形態に限定されない。当業者であれば、実施の形態で述べた構成に新たな構成要素を追加したり、削除したり、変更等したりして種々の変形を行うことができる。

【００７１】例えば、情報安全化装置２の提供する情報保証サービスが有料である場合等には、情報出力部１２から送信する情報を暗号化し、ユーザー端末１側でそれぞれ復号化するように構成することもできる。これにより、情報安全化装置２から複数のユーザー端末１に同一の情報を一斉に送信した場合でも、所定の暗号鍵を保有するユーザー端末１だけが情報を利用することができる。

【００７２】また、ユーザーは、複数の検査条件（規制ランク等）を予め設定することができ、時間帯や曜日等のパラメータに応じて検査条件を切り替えることも可能である。例えば、指定された曜日の指定されて時間帯については視聴規制を緩めたり、厳しくしたりすることができる。

【００７３】また、複数の置換用情報を用意しておき、ユーザーの希望に応じて情報の入れ替えを行うように構成することもできる。

【００７４】さらに、置換情報が用意されていない場合は、ソフトウエア又はハードウエアにより構成されたローパスフィルタを用いてオリジナル情報の低周波成分のみを抽出し、ユーザー端末１に送信するように構成することも可能である。あるいは、オリジナル情報の各フレームから動きのベクトルを抽出し、予め用意された代替オブジェクトを検出されたベクトルに基づいて動作させることにより置換情報を自動的に生成することもできる。

【００７５】さらに、前記実施の形態では、放送で送られてくる以外の情報と、放送で送られてくる情報とに分けて述べたが、それぞれで説明した情報の処理や情報の扱いは、送られてくる方式で区別する必要はない。

【００７６】また、情報安全化装置２とユーザー端末１とは、それぞれ別体に形成し分離配置する場合を例示したが、両者を一体化してもよい。

【００７７】

【発明の効果】以上詳述した通り、本発明によれば、情報端末は、事前に安全性が確認され、必要な処理が施された情報のみを受信することができ、使い勝手等が向上する。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る情報安全化装置を用いた情報保証システムの全体構成を概略的に示す構成説明図である。

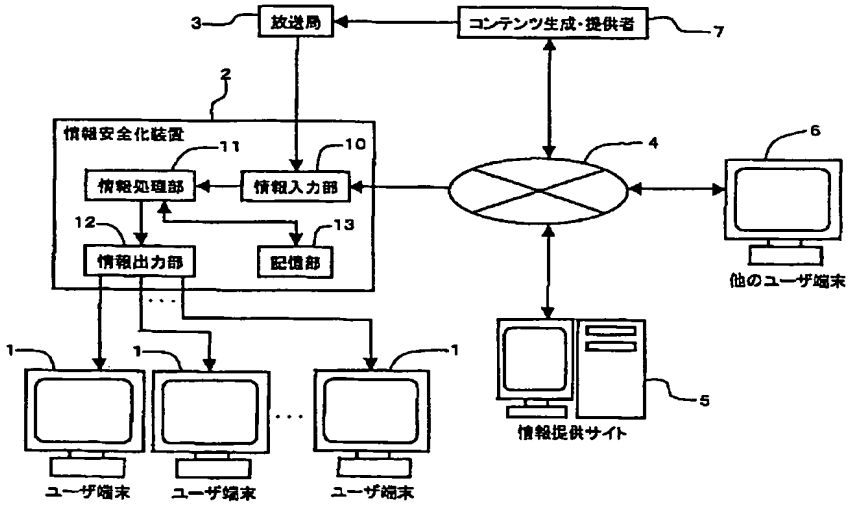
【図２】情報安全化装置の機能構成を示すブロック図である。

【図３】保証マークとコンテンツデータとの関係を示す説明図であって、図３（ａ）はデータ構造を示し、図３

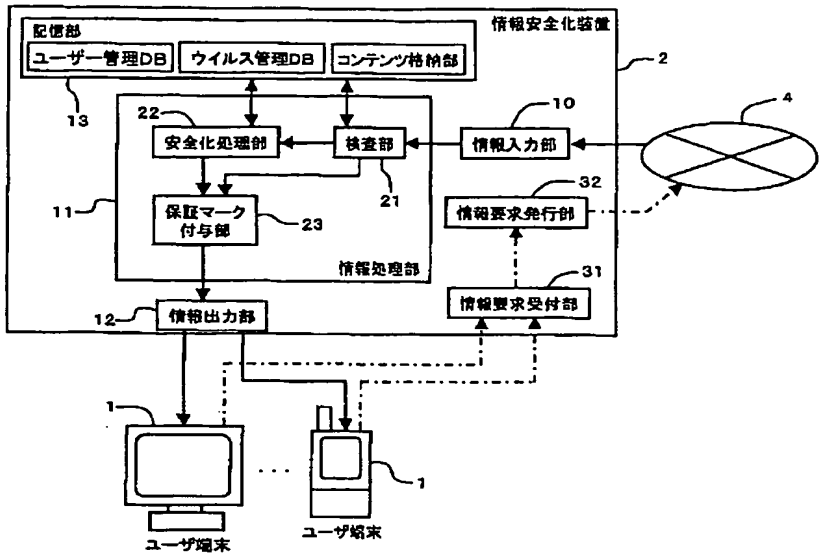
（ｂ）はユーザー端末側での表示例を示す。
【図４】視聴が規制されるべき場面を含んだコンテンツを再生する場合の説明図であって、図４（ａ）は置換用データに入れ替えずに再生する場合を、図４（ｂ）は置換用データに再生する場合をそれぞれ示す。
【図５】放送以外のデータとしてコンピュータウイルスを処理する場合の全体の流れを示す説明図である。
【図６】映画等の放送データを処理する場合の全体の流れを示す説明図である。
【図７】コンピュータウイルスを検査し処理する場合の概要を示すフローチャートである。
【図８】映画等の放送内容を検査し処理する場合の概要を示すフローチャートである。
【図９】ユーザー端末側の処理概要を示すフローチャートである。
【図１０】ユーザーの意思によって本情報保証サービスのセット、リセットが自由にできる状態を示す説明図である。
【図１１】情報安全化装置をインターネット接続事業者に適用した場合の説明図である。
＊【図１２】コンテンツ生成方法の概略を示す流れ図である。

【符号の説明】
１　ユーザー端末
２　情報安全化装置
３　放送局
４　通信ネットワーク
５　情報提供サイト
６　他のユーザー端末
７　コンテンツ生成・提供者の装置
１０　情報入力部
１１　情報処理部
１２　情報出力部
１３　記憶部
２１　検査部
２２　安全化処理部
２３　保証マーク付与部
３１　情報要求受付部
３２　情報要求発行部

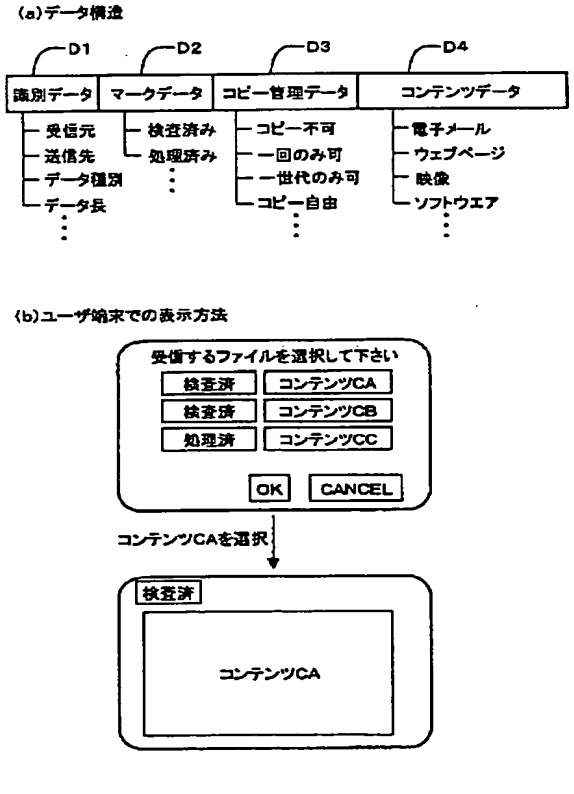
【図１】



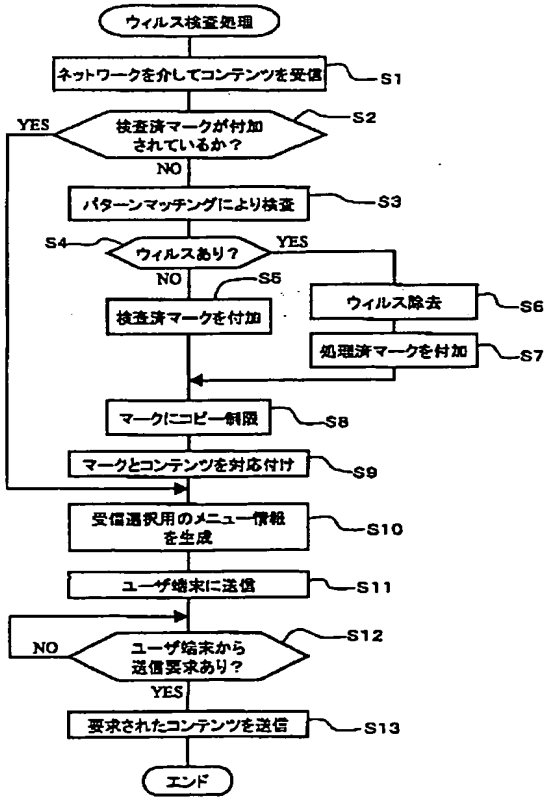
【図２】


記憶部
ユーザー管理DB
ウイルス管理DB
コンテンツ格納部
情報安全化装置
2
13
22
安全化処理部
検査部
10
情報入力部
4
21
11
保証マーク付与部
23
32
情報要求発行部
情報処理部
31
情報要求受付部
12
情報出力部
1
1
ユーザ端末
ユーザ端末

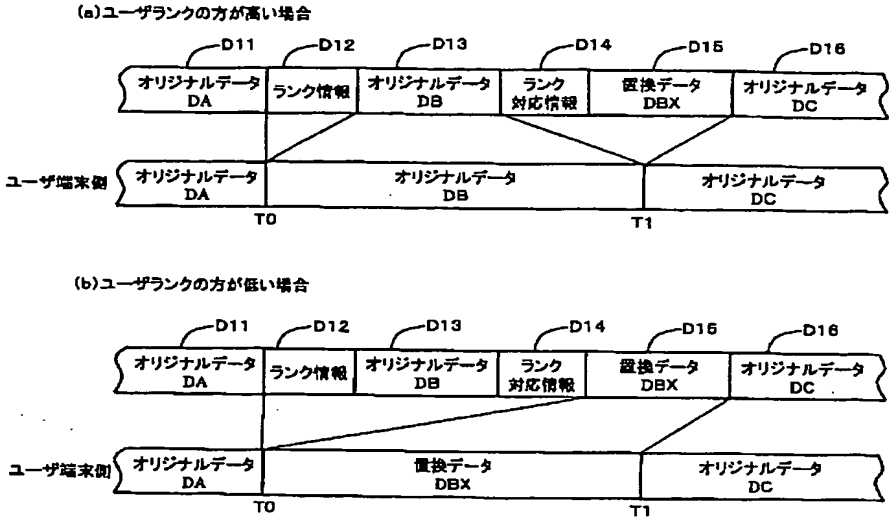
【図３】


(a)データ構造
D1
D2
D3
D4
識別データ
マークデータ
コピー管理データ
コンテンツデータ
受信元
送信先
データ種別
データ長
検査済み
処理済み
コピー不可
一回のみ可
一世代のみ可
コピー自由
電子メール
ウェブページ
映像
ソフトウエア
(b)ユーザ端末での表示方法
受信するファイルを選択して下さい
検査済
コンテンツCA
検査済
コンテンツCB
処理済
コンテンツCC
OK
CANCEL
コンテンツCAを選択
検査済
コンテンツCA

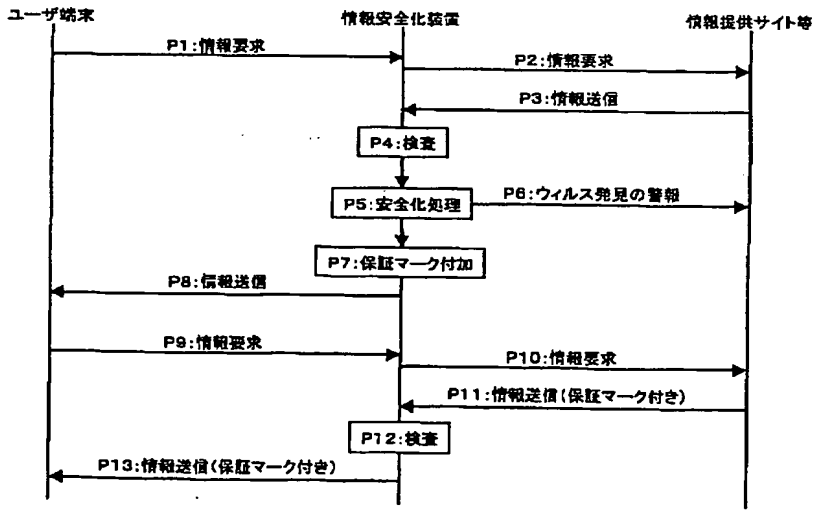
【図７】


ウィルス検査処理
ネットワークを介してコンテンツを受信
S1
YES
検査済マークが付加されているか？
S2
NO
パターンマッチングにより検査
S3
S4
ウィルスあり？
YES
NO
S5
検査済マークを付加
ウィルス除去
S6
処理済マークを付加
S7
マークにコピー制限
S8
マークとコンテンツを対応付け
S9
受信選択用のメニュー情報を生成
S10
ユーザ端末に送信
S11
NO
ユーザ端末から送信要求あり？
S12
YES
要求されたコンテンツを送信
S13
エンド

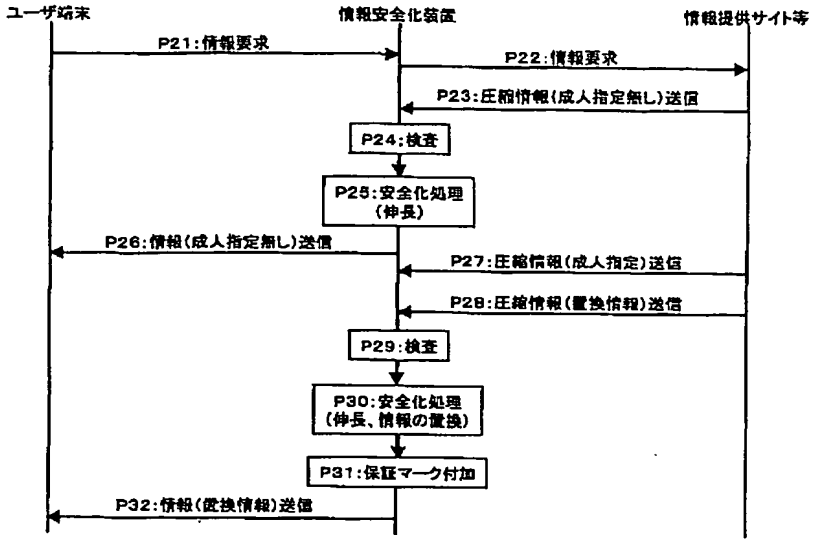
【図４】


(a)ユーザランクの方が高い場合
D11
D12
D13
D14
D15
D16
オリジナルデータ DA
ランク情報
オリジナルデータ DB
ランク対応情報
置換データ DBX
オリジナルデータ DC
ユーザ端末側
オリジナルデータ DA
オリジナルデータ DB
オリジナルデータ DC
T0
T1
(b)ユーザランクの方が低い場合
D11
D12
D13
D14
D15
D16
オリジナルデータ DA
ランク情報
オリジナルデータ DB
ランク対応情報
置換データ DBX
オリジナルデータ DC
ユーザ端末側
オリジナルデータ DA
置換データ DBX
オリジナルデータ DC
T0
T1

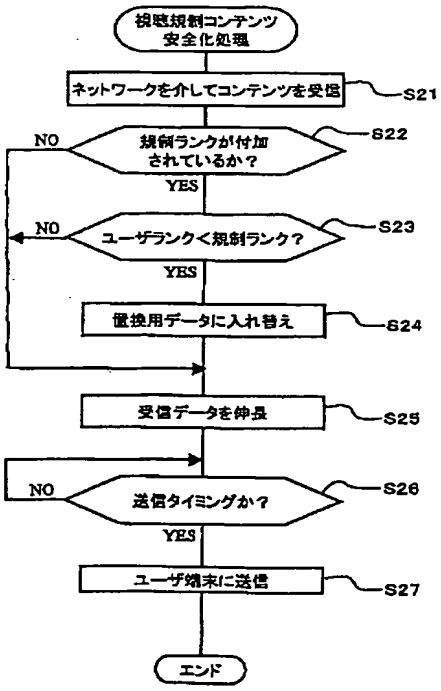
【図５】


ユーザ端末
情報安全化装置
情報提供サイト等
P1:情報要求
P2:情報要求
P3:情報送信
P4:検査
P5:安全化処理
P6:ウィルス発見の警報
P7:保証マーク付加
P8:情報送信
P9:情報要求
P10:情報要求
P11:情報送信(保証マーク付き)
P12:検査
P13:情報送信(保証マーク付き)

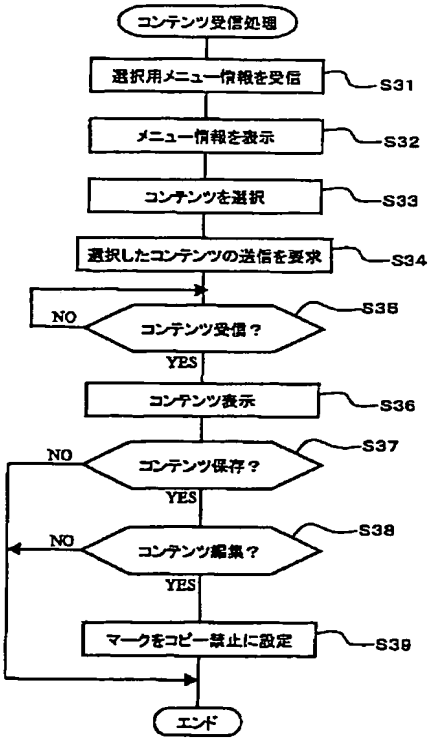
【図６】


ユーザ端末
情報安全化装置
情報提供サイト等
P21:情報要求
P22:情報要求
P23:圧縮情報(成人指定無し)送信
P24:検査
P25:安全化処理(伸長)
P26:情報(成人指定無し)送信
P27:圧縮情報(成人指定)送信
P28:圧縮情報(置換情報)送信
P29:検査
P30:安全化処理(伸長、情報の置換)
P31:保証マーク付加
P32:情報(置換情報)送信

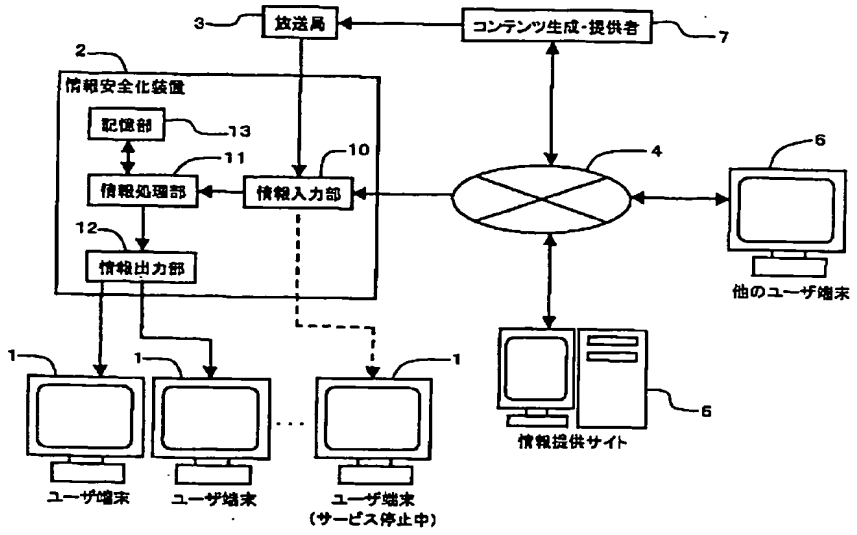
【図８】


視聴規制コンテンツ安全化処理
ネットワークを介してコンテンツを受信
S21
規制ランクが付加されているか？
S22
NO
YES
ユーザランク＜規制ランク？
S23
NO
YES
置換用データに入れ替え
S24
受信データを伸長
S25
送信タイミングか？
S26
NO
YES
ユーザ端末に送信
S27
エンド

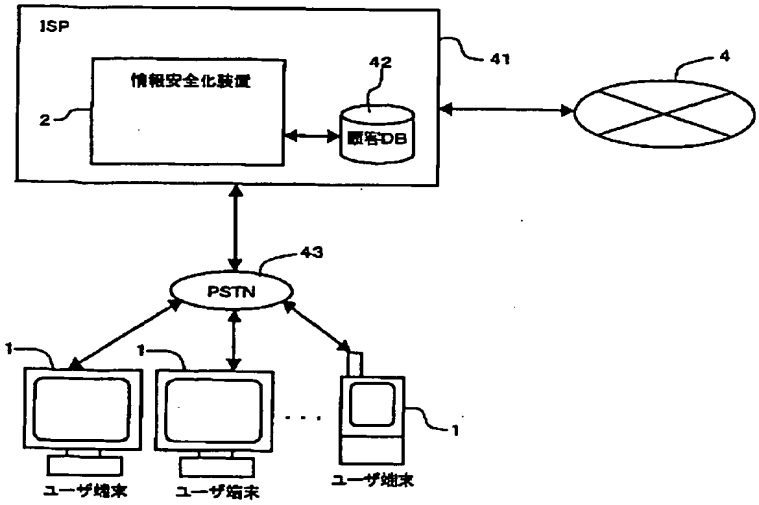
【図９】


コンテンツ受信処理
選択用メニュー情報を受信
S31
メニュー情報を表示
S32
コンテンツを選択
S33
選択したコンテンツの送信を要求
S34
コンテンツ受信？
S35
NO
YES
コンテンツ表示
S36
コンテンツ保存？
S37
NO
YES
コンテンツ編集？
S38
NO
YES
マークをコピー禁止に設定
S39
エンド

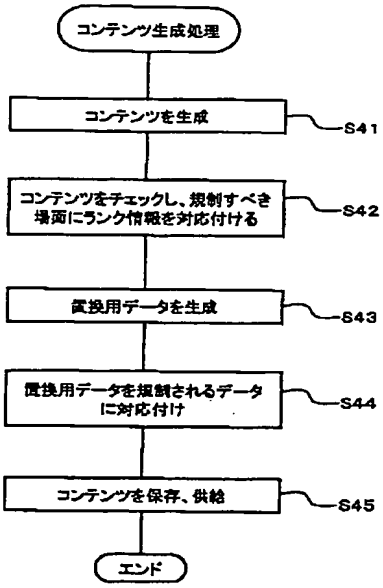
【図１０】


3
放送局
コンテンツ生成・提供者
7
2
情報安全化装置
記憶部
13
10
11
情報処理部
情報入力部
12
情報出力部
4
6
他のユーザ端末
1
1
1
ユーザ端末
ユーザ端末
ユーザ端末
（サービス停止中）
5
情報提供サイト

【図１１】


ISP
41
情報安全化装置
42
2
顧客DB
4
43
PSTN
1
1
1
ユーザ端末
ユーザ端末
ユーザ端末

【図１２】


コンテンツ生成処理
コンテンツを生成
S41
コンテンツをチェックし、規制すべき場面にランク情報を対応付ける
S42
置換用データを生成
S43
置換用データを規制されるデータに対応付け
S44
コンテンツを保存、供給
S45
エンド

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox